

Intrusion Detection Systems Adapted from Agent-based Artificial Immune Systems

Chung-Ming Ou

Department of Information Management
Kainan University
Luchu 33857, Taiwan
Email: cou077@mail.knu.edu.tw

Yao-Tien Wang

Department of Computer Science and
Information Engineering
Hungkuang University
Taichung 433, Taiwan
Email: ytwang@sunrise.hk.edu.tw

C.R. Ou

Department of Electrical Engineering
Hsiuping Institute of Technology
Taichung 412, Taiwan
Email: crou@mail.hit.edu.tw

Abstract—Agent-based artificial immune system (ABAIS) is applied to intrusion detection systems (IDS). A multiagent-based IDS (ABIDS) inspired by the danger theory of human immune system is proposed. The intelligence behind ABIDS is based on the functionality of dendritic cells in human immune systems and the danger theory, while dendritic cells agents (DC agent) are emulated for innate immune subsystem and artificial T-cell agents (TC agent) are for adaptive immune subsystem. Antigens are profiles of system calls while corresponding behaviors are regarded as signals. This ABIDS is based on the dual detections of DC agent for signals and TC agent for antigen, where each agent coordinates with other to calculate danger value (DV). ABAIS is an intelligent system with learning and memory capabilities. According to DVs, immune response for malicious behaviors is activated by either computer host or Security Operating Center (SOC).

Multiple agents are "embedded" to ABIDS, where agents coordinate one another to calculate mature context antigen value (MCAV) and update activation threshold for security responses. Accordingly, computer hosts met with malicious intrusions can be effectively detected via input signals and temporary output signals such as PAMP, danger and safe signals.

Index Terms—intrusion detection, multiagent, artificial immune systems, dendritic cell algorithm

I. INTRODUCTION

The Internet has become a major environment for propagating malicious codes, in particular, through web applications. Internet worms spread through computer networks by searching, attacking and infecting remote computers automatically. Intrusions, in particular, web-based ones, have become increasing threats for information assets. In order to defend against network attacks, one efficient way is to understand various properties of virus, which include the impact of patching, awareness of other human countermeasures and the impact of network traffic, even the ways how these malicious codes reside in a certain hosts, etc.

Forrest et al. [1] proposed an instance of computer immunology to protect the computer systems using the principles of human immune systems. Gu et al. [2] proposed an architecture of combining multiagent systems and dendritic cells. Most AIS researches focus on the development of specialized AIS algorithms inspired by theories such as the negative selection theory or the danger theory. Applying AIS algorithm to IDS can be traced back to [3].

Greensmith et al. [4] employed dendritic cells (DCs) within AIS which coordinate T-cell immune responses. Kim et al. [5] proposed "CARDINAL" which embedded T-cell process within the danger-theory-based AIS. Greensmith et al. [4], [6] proposed the Dendritic Cell Algorithm (DCA) whose purpose is to correlate data in the form of antigens and signals, then to identify groups of antigens as normal or anomalous. DCA achieves such missions through a generation of an anomaly coefficients, namely, *mature context antigen value (MCAV)*. It is believed that a DC is better performed by agent technology while considering its adoption to network environment. This antigen-plus-context information is passed on to a class of responder cells, termed T-cells. DCs are natural intrusion detection agents, which monitor the host tissue for evidence of cell damage. DC agents in our agent-based intrusion detection system (ABIDS) will evaluate antigens and corresponding signals according to DCA to determine whether antigens are malicious nor not.

For information security, one important aspect learned from immunology is the following: a computer security system should protect a host or network of hosts from unauthorized intruders, which is analogous in functionality to the immune system protecting the body from invasions by foreign pathogens. For example, anti-virus software has recently adopted some features analogous to the innate immune system, which can detect malicious patterns. However, most commercial products do not yet have the adaptive immune system's ability to address novel threats.

The motivation of this research is the following. Can agent-based information security systems learn itself to effectively determine whether the abnormality is "actually" incurred by some malicious attacks? This paradigm is very similar to the danger theory proposed in the immunology [7]. The arrangement of this paper is as follows. In section 2, preliminary knowledge such as AIS, danger theory, intelligent agents system and computer security are introduced. For section 3, IDS based on ABAIS model inspired by DT is discussed. Simulations of two agent-based algorithms for ABIDS based on different scenarios will be given in section 4.

II. BACKGROUND

A. Intrusion Detection Systems (IDS)

Intrusion detection systems (IDS) focus on exploiting attacks, or attempted attacks, on networks and systems, in order to take effective measures based on the system security policies, if abnormal patterns or unauthorized access is being suspected. However, there are two potential mistakes by IDS, namely, false positive error (FPE) and false negative error (FNR). For FPE (FNE), a pattern is mistakenly determined as abnormal (normal).

The main goal of IDSs is to detect unauthorized use, misuse and abuse of computer systems by both systems insiders and external intruders. It can be a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. A host-based intrusion detection system (HIDS) consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. It is an crucial issue of establishing principles of designing an IDS. According to [5], there are three such principles as follows.

- 1) Types of system response should be determined by attack severity and certainty.
- 2) For performing adequate magnitudes of responses, both local and peer information needs to be taken into account.
- 3) Optimize the number of peer hosts polled.

B. Human Immune System (HIS)

The human immune system (HIS) consists of the antibodies and lymphocytes, which include T-cells and B-cells. HIS uses a large number of highly specific B- and T-cells to recognize antigens. Only B-cells secrete antibodies. Clonal selection theory explains the details of antibody secretion specific to an antigen where T-cells help regulating. The binding between antigen and specific lymphocytes trigger proliferation from immature lymphocytes to mature one and the secretion of antibodies.

HIS can be categorized as innate and adaptive immune system. The innate immune system is characterized by three roles, namely, host defense in the early stages of infection, induction of the adaptive immune response and determination of the type of adaptive response through antigen presenting cells (APCs) [8]. On the other hand, the main characteristics of the adaptive immune system are recognitions of pathogens.

1) *Dendritic Cells*: The dendritic cell (DC) is a vital link between the innate and adaptive immune system and provides the initial detections of pathogenic invaders. DC is an APC which captures antigen protein from the surrounding area and processes it by ingesting and digesting the antigen. DCs are also part of innate immune system; once activated, they migrate to the lymphoid tissues where they interact with T-cells and

B-cells to initiate the adaptive immune response. Moreover, adaptive immune response is "orchestrated" by DCs.

DCs are the first defense line for HISs which will arrive at the locations where antigens intrude and then swallow the latter to the pieces. These pieces will be attached to APCs and presented to the T-cells. DCs can be regarded as the commanders for HISs; they can combine the danger and safe signal information to decide if the tissue environment is in distress or is functioning normally.

2) *T-Cell*: DCs will influence the differentiation of T-cells by releasing particular cytokines. In other words, DCs drive the T-cell to react to the antigen in an appropriate manner. Naive T-cells are those who have survived the negative and positive selection processes within the thymus, and have migrated to circulation system between the blood and lymphoid organs where they wait antigen presentation by DC's. Naive T-cells reach an activated state when the T-cell receptor (TCR) on their surfaces binds to the antigen-peptide-MHC molecules on the surfaces of DC's, and co-stimulatory molecules are sufficiently upregulated on the surface of the DCs to show the degree of danger signals. The activated T-cells proliferate and their clones will differentiate into other cells such as helper t-cell and cytotoxic T-cells (CTL).

C. Artificial Immune Systems

Artificial Immune Systems (AIS), which is based on HIS, have been applied to anomaly detections [2][3][5][9][10]. AISs have been developed according to negative selection algorithm and clonal selection algorithm which are based on the classical self-nonself theory; nonselfs are entities which are not part of human organisms. This so-called self-nonself classification theory had been challenged while failing to explain several immunological phenomena. Some alternative theories have been proposed, for example, the danger theory (DT). DT postulates that the human immune systems respond to the presence of molecules known as danger signals, which are released as results of unnatural cell deaths.

D. Danger Theory (DT)

Matzinger [7] proposed the Danger Theory, which has become more popular among immunologists in recent years for the development of peripheral tolerance (tolerance to agents outside of the host). DT states that the immune system will only respond when damage is indicated and is actively suppressed otherwise. DT proposes that APCs, (in particular, DCs), have danger signal receptors (DSR) which recognize signals sent out by distressed or damaged cells. These signals inform the immune systems to initiate immune responses. APCs are activated via the danger signals. These activated APCs will be able to provide the necessary signals to the T-cells (more precisely, T-helper cells) which control the adaptive immune response.

Danger signals are generated by ordinary cells of the body that have been injured due to attacks by pathogens. These signals are detected by DCs. There are three modes of operation: immature, semi-mature and mature. In the DC's immature

state, it collects antigens along with safe and danger signals from its local environment. DC is able to integrate these signals to decide whether the environment is safe or dangerous. If it is safe, DC becomes semi-mature. Upon presenting antigens to T-cells, DC will cause T-cells tolerance. If it is dangerous, DC becomes mature and causes the T-cells to become reactive on antigen-presentations.

E. Agent-based Artificial Immune Systems

Agent is an entity that has the ability of consciousness, solving problem, self-learning and adapting to the environment, which is very similar to immune systems in functionalities. Table I summaries such similarities between AIS and multiagent systems (MAS). Accordingly, AIS can be contributed to the learning mechanism of agents: the immune system response attributes of specificity, diversity, memory and self/non-self recognition are needed. It may be used to optimize the agent's responses to intruders. Functionalities of the biological immune system, such as content addressable memory, adaptation, etc., can be utilized in intelligent agents.

TABLE I
COMPARISONS BETWEEN MAS AND AIS

System	MAS	AIS
Diversity Generation	Yes	Yes
Self Tolerance	Yes	No
Learning	Yes	No
SNS Act. Threshold	Yes	Yes
Self Maintenance	Yes	Yes
Short-term Memory	Yes	Yes
Long-term Memory	Yes	No

Adaptiveness is a challenge and also an important feature for MAS to interact with the environment. Three major stages for ABAIS inspired by the clonal selection theory are diversity generation, self-maintenance and memory of nonself. The last two properties define the adaptiveness of the IBMAS. These steps are carried out by agents distributed over the MAS.

- **Diversity Generation:** Continuous diversity generation leads to the "adaptation" of ABAIS. Diverse agents with distinct specificity of the receptor and the effector are generated by way of mutations.
- **Self-Maintenance:** Agents are adjusted to be insensitive to known patterns (self) during the developmental phase. Negative selection theory is a central of this phase.
- **Memory of Nonself:** Agents are adjusted to be more sensitive to unknown patterns (nonself) during the working phase.

III. INTRUSION DETECTION MECHANISM BASED ON ABAIS

According to [10][11][12], we propose improved IDS based on ABAIS, or ABIDS in short. Different from traditional self-nonsel self paradigm for immune systems, our IDS will first detect danger signals emitted by computer hosts. These danger signals are based on some security threat profile, which defines by system calls generated by running processes. According to

[9][11], threat profile may be composed of excessive CPU, memory load at the host, bandwidth saturation, high connection number of the host, etc. In this multi-agent system, several agents are generated which can communicate each other to emulate functionalities extracted from DT-inspired AIS (Fig 1).

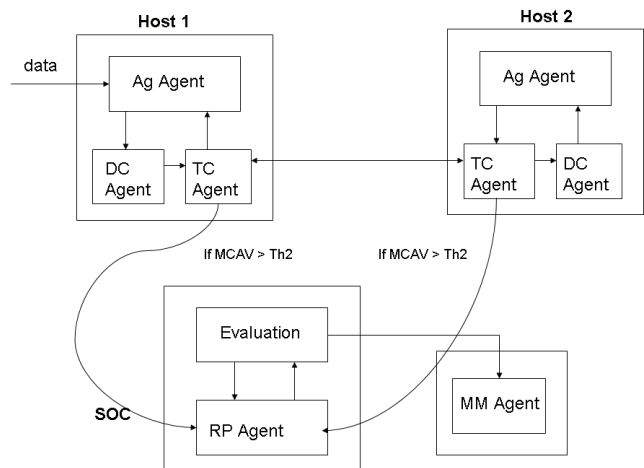


Fig. 1. Architecture of ABIDS.

A. Antigen

For most network detecting systems (for example, those adopting self-nonself paradigm), an antigen is defined as an information vector extracted from network packet. For example, antigens are binary strings extracted from the IP packets, which include IP address, port number, protocol types, etc. However, the antigen defined at Our ABIDS is related to system calls rather than network packets. A system call is the way how a program requests a service from an operating system's kernel. System calls provide the interface between a process and the operating system. Each process invokes some system calls. The more active the process, the more system calls it makes. Each system call is captured and converted into an antigen [13].

B. Intelligent Agents in AIS

We design a MAS with antigen agents, DC agents, T-Cell agents, Responding agents and Memory agents to perform functionalities of ABIDS such as DCAs, antigen memorization, etc.

1) *Antigen Agent (Ag Agent)*: Antigen agents, which are installed at computer hosts, represent data item from the nonself dataset. They extract and record selected attributes from these data items. According to the agent-based DCA (ABDCA) which will be described later, each Ag agent sends corresponding DC agent a picked message when a nonself antigen appears.

2) *Dendritic Cell agent (DC agent)*: In order to determine whether a malicious behavior is taking place, ABIDS needs to analyze antigens. DC agents are the kernel of the ABAIS which are complex compared to other agents; they are installed and distributed at each computer hosts. When an Ag agent issues a picked signal, corresponding DC agent will evaluate the risk

state facing by the host by calculating the danger value (DV). Similar to nature DC, each DC agent has three stages, namely immature, semimature and mature. DC agents are started from immature stages. When a picked signal issued from the Ag agent, DC agent executes data processing function such as the ABDCA. When a DC agent is at either semimature state or nature state, it returns the mature context to corresponding TC agent.

3) *T-cell agent (TC Agent)*: TC agents are also installed at each computer hosts. TC agents are activated by the signals from DC agents when the DVs exceed thresholds. Each TC agent have three numerical values associated with it; these represent the accumulated certainties and severities of attack: *T-cell activation threshold*, *Th1 activation threshold*, *Th2 activation threshold*. These TC agents will communicate each other for exchanging these numerical values. There are two perspectives of this agent communications.

- For TC agent issuing malicious act warning for corresponding antigen, it informs TC agents "nearby" by exchanging its numerical values.
- For TC agent not issuing malicious act warning for this antigen, it simply update its numerical values according "nearby" TC agents issuing malicious act warning.

4) *Responding Agent (RP agent)*: Ag agents, DC agents and TC agents are coordinating one another to perform malicious act responses. After DV exceeds threshold value, TC agents will inform RP agent, which is installed at SOC and each computer host. RP agents will activate some control measure to such malicious act. Two measures are considered:

- 1) Reporting to the SOC or security manager, for example, patches downloaded, activate relevant anti-virus software on this infected host and removes virus.
- 2) Disruption of intrusion, discards a suspicious packets, kill the related process, cut-off infected sub-network. These can prevent large-scale spreading of computer viruses, in particular internet worms, which have high spreading rate by their natures.

C. Algorithm: Agent-based Dendritic Cell Algorithm (ABDCA)

If an antigen is collected in an environment of danger, the context of this antigen is marked as anomalous and such antigen collected by the DC agent is potentially an intruder. While in the immature state, DC agent performs the following three functions:

- 1) Antigen Sampling: DC agents collect antigens from some external sources (in this case, from computer hosts) and places these antigens in its own antigen storage.
- 2) Update input signals: DC agent collect values of all input signals present in the signal storage area.
- 3) Calculate interim output signals: each DC agent calculates its three temporary output signal values from the received input signals, then derives its final output signal.

We observe that multiple DCs present multiple copies of the same antigen type for invoking an immune response; it leads

to an error-tolerance immune system as a single DC is far from stimulating a "false positive" error. The ABDCA is listed as follows.

Algorithm 1 Agent-based DCA (ABDCA)

```

input : Antigens and signals
output: Antigen context (0 for safe/1 for danger)
Initialize DC agents (Immature state);
for each DC_agent_i do
  get antigen (Ag);
  store antigen;
  get input_signal;
  calculate output_signal_i;
  if output_signal_i > Activation_Threshold_i then
    Ag_context is assigned as 0;
    State of DC_agent_i="semi-mature";
  else
    Ag_context is assigned as 1;
    state of DC_agent_i="mature";
  end if
end for
update cumulative output_signals;

```

Three temporary output signals are PAMP signal, danger signal and safe signal. According to Greensmith et al. [13], the system should respond with a very high rate of false positives by switching the PAMP and safe signal. The definitions of PAMP, danger and safe signals, by way of parameters of computer hosts such as CPU usage, memory load, network connection (number) and bandwidth saturation, are as follows.

- 1) PAMP Signal: Network Connection > th_netconnection AND bandwidth Saturation > th_bandsaturation.
- 2) Danger Signal: CPU Usage > th_cpuload OR Memory Load > th_memoryload.
- 3) Safe Signal: All parameters < th_parameter.

Where "th_parameter" represents the threshold value of the parameter. Now the computation of output signals by three temporary output values is the following.

$$output_signal = \frac{W_P \cdot C_P + W_D \cdot C_D + W_S \cdot C_S}{W_P + W_D + W_S} \quad (1)$$

According to empirical experiments [4], the weights for this output signal is $W_P = 2$, $W_D = 1$, $W_S = 1$. C_P , C_D , C_S represent PAMP signal, danger signal and safe signal. The principle for this weights is the following: PAMP signal will decide whether the danger signal will be a "really" harmful one. Whether output signal is harmful or nor is defined by the Table II.

TABLE II
DEFINITIONS OF OUTPUT SIGNAL.

Output Signal	C_P	C_D	C_S
Normality	0	0	1
Harmless Abnormality	0	1	0
Harm Abnormality	1	1	0

D. Algorithm: Agent-based IDS

Now according to ABDCA, we propose an algorithm describing agent-based IDS. This algorithm is also illustrated as Fig. 2. ABDCA can provide information not only a network packet but also a group of network packets is anomalous or not. This is achieved by the generation of an anomaly coefficient value, namely MCAV.

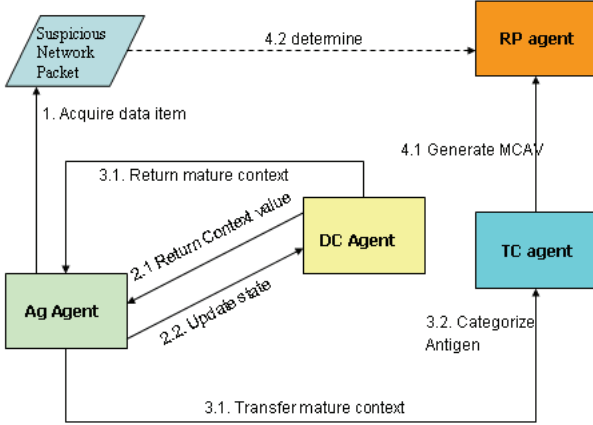


Fig. 2. Diagrammatic Illustration of Agent-based intrusion detection system.

Algorithm 2 Agent-based IDS (ABIDS)

Input: Antigen and Signals

Output: Antigen Types

1. Data Processing:

1.1 Ag agent extracts antigen from network traffic signal according to ag agent attribute.

2. Agent response:

2.1 DC agent returns context value according to threat profile; also according to the policy of the SOC if necessary.
2.2 DC agents will response to such antigen by updating its state according to DCA.

3. Danger Signal processing:

3.1

if this DC agent returns mature values to Ag agent **then**
 Ag agent transfers it to the TC agent.

end if

3.2 TC agent categorizes such antigen according to the(updated)threat profile.

4. MCAV generation:

4.1 TC agent generates MCAV, which is sent to the RP agent.

4.2 RP agent determines if the corresponding antigen is malicious or not.

5. Antigen Memory:

5.1 Memory Agent stores necessary MCAV information

For the step 4 of the Algorithm 2, each nonself antigen gets a binary string of mature contexts from every selected DC agent installed at corresponding computer host. MCAV can be calculated through the number of context "1" divided by the number of all contexts. According to [2], it is similar to a voting system, where the antigen is the candidate and the DC agents are the voters. If the context is "1" ("0"), it means the DC agent determines this antigen is malicious (benign). The MCAV is actually the probability of that this antigen is being malicious.

The reactions of RP agents can be multiple according to the SOC's security policies. For example, passive reaction is initiated by sending some alarm signal such as an e-mail to the administrator and a strategy proactive is defined through mobile agents that implement the characteristics of the reaction. According to [11], for example, an applied reaction is defined for each of the following internet protocols such as DNS, FTP, HTTP, POP3 and SMTP. The issue of RP agents is out of the scope of this paper.

E. Agent Communications

One advantage of ABIDS is the communications and co-ordination between DC agents and TC agents. The basic idea is as follows. TELL and ASK-based communication permit agents share their internal information, enhancing their performances to respond to intruders [10]. On the other hand, useful knowledge obtained by DC agents and TC agents should be stored in some databases. These databases could also be shared by each DC and TC agent to improve their detection efficiencies. Suitable mechanisms of agent communications can contributed to better performance of ABIDS.

On the other hand, if a TC agent determines its host is under malicious attack by analyzing the corresponding MCAV, it will inform other TC agent "nearby". Such communication is direct and does not pass through proxy server or SOC. The activation threshold of this TC will be updated according to the following equation.

$$T(t) = T(t-1) + \alpha E(t-1)(E(t-1) - T(t-1)), t = 1, 2, \dots, t_b \quad (2)$$

where E_i is the excitation level of TC agent, and t_b is the attacking time by this antigen.

Table III and Table IV illustrate the agent communications [14].

TABLE III
AGENTS AND THEIR COMMUNICATIONS (1).

Communication	Initiator	Receiver
eRaiseWarning	Ag Agent	DC agent
eContextReturned	DC Agent	TC Agent
eMaliciousOrNot	DC agent	TC agent
eEvidenceResponse	TC Agent	RP agent
eMemoryInitiation	RP agent	Memory Agent

TABLE IV
AGENTS AND THEIR COMMUNICATIONS(2).

Communication	Description
eRaiseWarning	Notify of a possible malicious attack
eContextReturned	sending MCAV
eMaliciousOrNot	Identify the malicious antigen
eEvidenceResponse	Implement the system response according to TC agent's information
eMemoryInitiation	Memorize the nonself antigen being encountered; update antigen database of Proxy server

F. Agent Platform

One advantage of this ABIDS is the following: it is feasible to be adapted into large-scale computer networks such as cloud computing environment, as TC agents will collect information from computer hosts to calculate MCAVs, and also update threat profile if necessary. Fig. 3 illustrates the agent interactions between SOC and computer hosts on agent platforms.

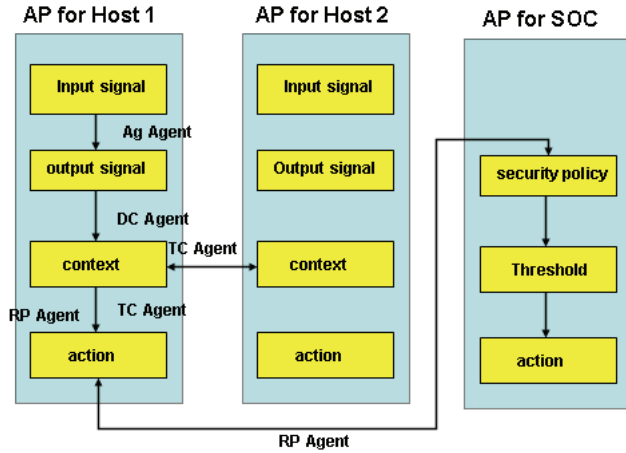


Fig. 3. Agent Interaction for ABIDS.

Table V and Table VI are the comparisons for goals and services fulfilled by these agents.

TABLE V
AGENTS, GOALS AND SERVICES (1).

Agent	Goals
Ag Agent	Data Parsing
DC Agent	Detect malicious codes or network attacks at the input sources
TC Agent	Categorize nonself antigen
RP Agent	Reduce the malicious antigen
Memory Agent	Memorize the nonself antigen

TABLE VI
AGENTS, GOALS AND SERVICES (2).

Agent	Services
Ag Agent	antigen label and signal association
DC Agent	MCAV estimation, update activation threshold
TC Agent	Identify the malicious antigen
RP Agent	Implement the system response
Memory Agent	Update the antigen database of the proxy server

IV. SIMULATION

A. Malicious Behaviors determined by ABDCA

According to essence of the danger theory, the advantage of ABIDS is the following: it can determine some nonself-antigenic behavior which is at the verge of normality and abnormality. For example, for those network behaviors with short attacking time. In this section, we simulate several critical cases for this ABIDS. The threshold of S , C and T are the following $S_{th} = 0.50$, $C_{th} = 0.50$ and $T_{th} = 0.5$. The number of computer hosts within this network is 2000. Each host has its fixed vector of weights. Simulation principle is to determine those critical behaviors, which include one extremely high factor with other low factors, or some factors are closing to the corresponding threshold values.

1) *Nonself Antigen with High Severity, Low Certainty and Short Attacking Time*: While an antigen intrudes a computer host with behaviors of high severity but low certainty and short attacking time, it is difficult sometimes to determine if this is a malicious attack. In this case, we consider the threat profile $TP=[0.9, 0.01, 0.01]$ for the ABDCA algorithm.

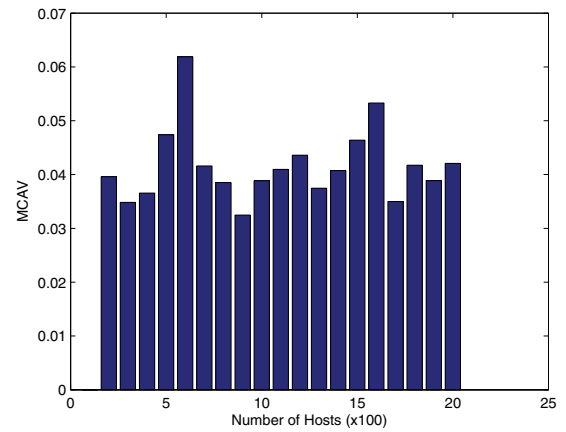


Fig. 4. Average MCAV for an Antigen with High Severity solely.

We expect the simulation should be "stable" for reasonable many hosts as Fig. 4. MCAV is around 0.03 and 0.05, which shows that this nonself antigen is normal.

2) *Nonself Antigen with Edge Behavior*: While an antigen intrudes a computer host with edge behavior such that severity, certainty and attacking time are all closing to their threshold values, respectively. It is also difficult to determine if this is a malicious attack or not. In this case, we consider $TP=[0.65, 0.65, 0.65]$.

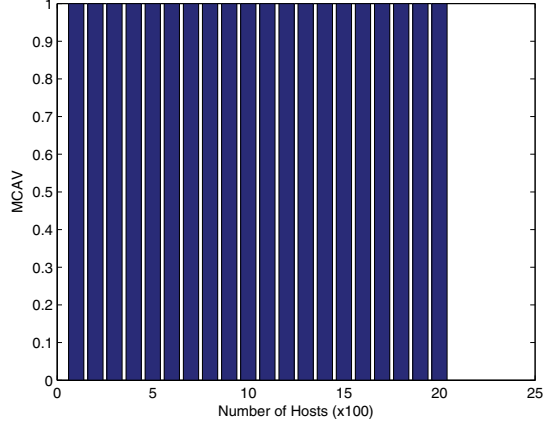


Fig. 5. Average MCAV for an Antigen with Critical Threshold Behavior.

The simulation also show a stable result (see Fig. 5); average MCAV is equal to 1, which indicates that this nonspecific antigen is harmfully abnormal.

3) *Nonspecific Antigen with Short Time Attack*: In this simulation, an antigen causes computer hosts with both high severity and certainty, but relative medium attacking time. It is difficult to determine if this is a malicious attack or not. In this case, we consider $TP=[0.9, 0.9, 0.4]$.

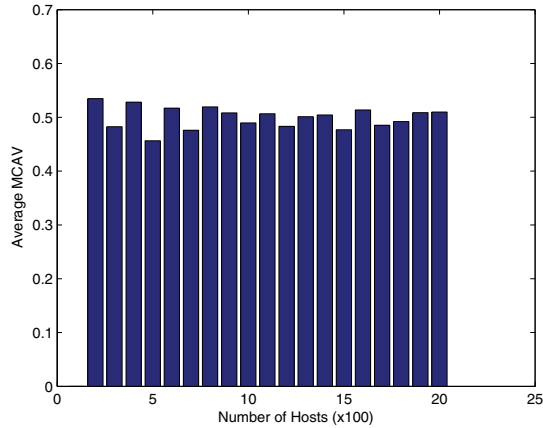


Fig. 6. Average MCAV for an Antigen with High Severity and certainty, but relatively short Attacking Time.

The simulation show a stable result (see Fig. 6); average MCAV is around 0.5, which indicates that this nonspecific antigen can be harmfully or harmful abnormal depending on the SOC's security profile.

B. Simulation of TC Agents' Coordinations

1) *Interactions between Two TC Agents*: We consider two computer hosts with TC interactions. TC1 and TC2 are informing each other for confirmed attack from the corresponding antigen.

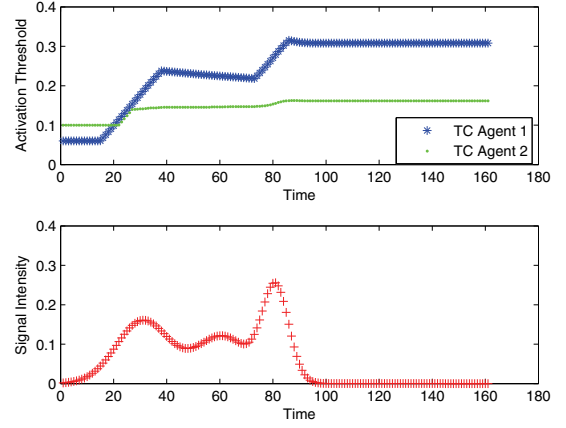


Fig. 7. Activation Thresholds of Two TC agents within the attacking cycle.

According to Fig. 7, even two TC agents will lead to "more" complex threshold behaviors.

2) *Interactions among Three TC Agents*: We consider three computer hosts with TC agents interactions. TC1, TC2 and TC3 are informing each other for confirmed attack from the corresponding antigen.

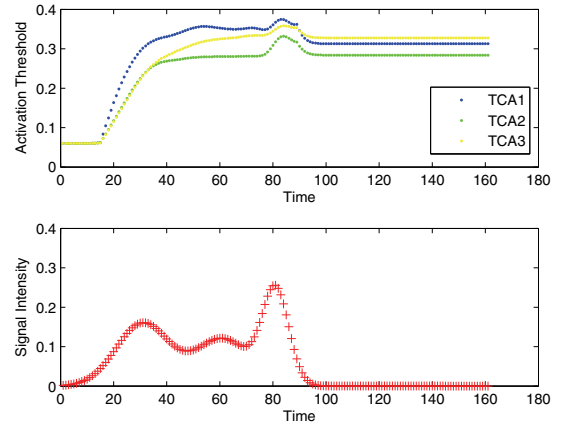


Fig. 8. Activation Thresholds of Three TC agents within the attacking cycle.

V. CONCLUSION

We propose a multiagent-based intrusion detection system. The intelligence behind such system is based on the danger theory of human immune systems. In particular computations of danger values with dynamic thresholds will reduce the false positive rate of danger signals issued by computer hosts. Three agents, namely, Ag agent, DC agent and TC agents are

coordinated to exchange information of intrusion detections. The evaluations of three factors S, C, and T are pragmatic issues. On the other hand, threshold values have to be defined by SOC's according to security profiles.

REFERENCES

- [1] S. Forrest, A. Hofmeyr, T. Somayaji, and Longstaff, "A sense of self for unix processes," in *Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy*, 1996, p. 120V128.
- [2] F. Gu, U. Aickelin, and J. Greensmith, "An agent-based classification model," in *9th European Agent Systems Summer School (EASSS2007)*, 2007.
- [3] U. Aickelin, P. Bentley, S. Cayzer, and J. Kim, "Danger theory: The link between ais and ids," *Lecture Notes in Computer Sciences*, vol. 2787, pp. 144–165, 2003.
- [4] J. Greensmith, J. Feyereisl, and U. Aickelin, "The dca: Some comparison," *Evolutionary Intelligence*, vol. 1, no. 2, pp. 85–112, 2008.
- [5] Kim, *An Artificial Immune System Architecture for Computer Security Applications*. New York: John Wiley and Sons, 1978.
- [6] J. Greensmith, U. Aickelin, and S. Cayzer, "Detecting danger: The dendritic cell algorithm," *Robust Intelligent Systems*, vol. 12, pp. 89–112, 2008.
- [7] P. Matzinger, "Tolerance, danger and the extended family," *Annual Review in Immunology*, vol. 12, pp. 991–1045, 1994.
- [8] K.-W. Yeom and J.-H. Park, "An artificial immune system model for multi agents based resource discovery in distributed environments," in *Proceedings of the First International Conference on Innovative Computing, Information and Control*, 2006, pp. 234–239.
- [9] J. Zhang and Y. Liang, "Integrating innate and adaptive immunity for worm detection," in *Proceedings of the Second International Workshop on Knowledge Discovery and Data Mining*, 2009, pp. 693–696.
- [10] H. Fu, X. Yuan, and N. Wang, "Multi-agents artificial immune system (maais) inspired by danger theory for anomaly detection," in *2007 International Conference on Computational Intelligence and Security Workshops*, 2007, pp. 570–573.
- [11] A. Boukerche, R. Machado, K. Juca, J. Sobral, and M. Motare, "An agent based and biological inspired real-time intrusion detection and security model for computer network operations," *Computer Communications*, vol. 20, pp. 2649–2660, 2007.
- [12] J. Kim, *Integrating artificial immune algorithms for intrusion detection*. University College London: Ph. D thesis, 2002.
- [13] J. Greensmith, U. Aickelin, and G. Tedesco, "Information fusion for anomaly detection with the dendritic cell algorithm," *Information Fusion*, vol. 11, no. 1, pp. 21–34, 2010.
- [14] P. Harmer, P. Williams, G. Gunsch, and G. Lamont, "An artificial immune system architecture for computer security applications," *IEEE Transactions on Evolutionary Computations*, vol. 65, no. 3, pp. 252–280, November 2002.